Attribute Measurement System with Information Barrier (AMS/IB)—Conceptual Description

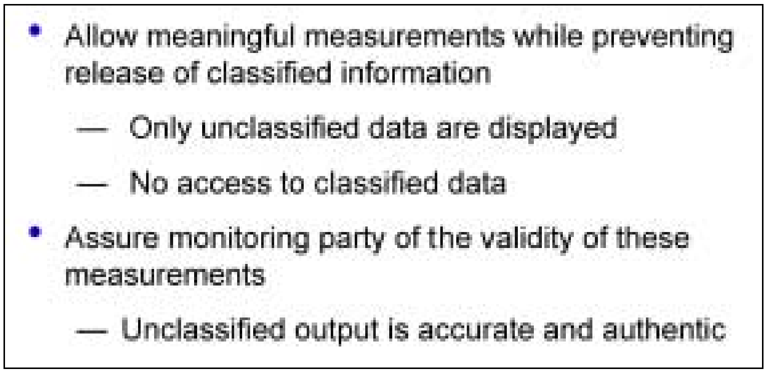
Duncan W. MacArthur
Los Alamos National Laboratory

Abstract

This paper is intended as a companion piece to the set of viewgraphs of the same name that was presented at the Fissile Material Transparency Technology Demonstration (FMTTD), which was held in Los Alamos in August 2000. These viewgraphs describe the concept of an information barrier as well as specific design criteria relating to the attribute measurement system with information barrier (AMS/IB) demonstrated in the FMTTD. Of particular interest are: design features and types of controls, the core concept of this information barrier (IB) design, the issues of inspectability and authentication, and the elements and integration of the AMS/IB itself.

Information Barriers

The goals of any information barrier system (Fig. 1) are twofold. The first is to ensure the protection of the host country's classified data and display only unclassified information. The second goal is to assure the monitoring party that these unclassified outputs are accurate, authentic, and have a direct causal relationship with the (unseen) classified measurements.

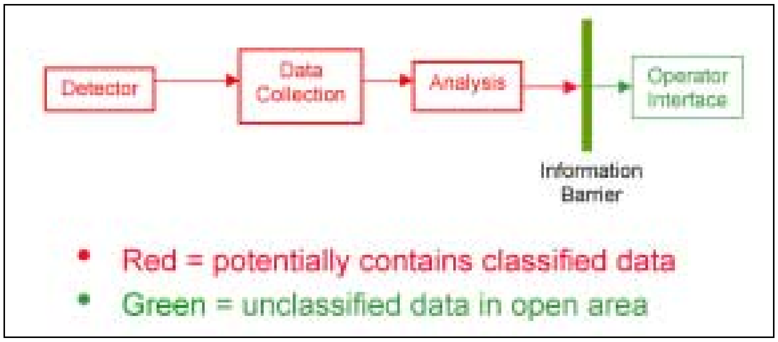


- Allow meaningful measurements while preventing release of classified information
  — Only unclassified data are displayed
  — No access to classified data
- Assure monitoring party of the validity of these measurements
  — Unclassified output is accurate and authentic

Fig. 1. Goals of an information barrier.

Although the first constraint is absolute, the second constraint is also essential to the design of an acceptable information barrier. Thus, neither one can be "traded off" against the other.

A conceptual measurement system with IB (Fig. 2) consists of one or more standard data acquisition systems (neutron and/or gamma) with an "IB" stripe pasted across them to separate the classified measurements from the unclassified outputs. In this design, standard nondestructive assay (NDA) techniques are used for the detection systems, so no detector research should be required. The remainder of this paper deals with the specifics of designing a workable "IB stripe."

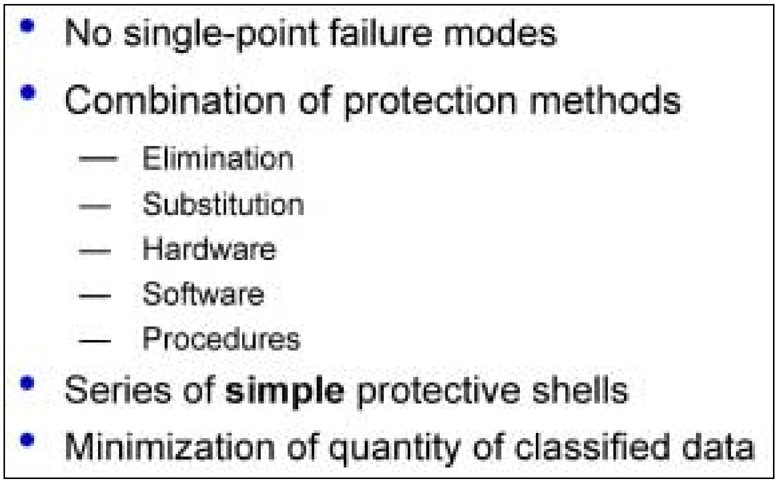


- Red = potentially contains classified data
- Green = unclassified data in open area

Fig. 2. Conceptual measurement system with IB.

Design of the AMS/IB

A very important feature of the AMS/IB design is "defense-in-depth" (Fig. 3). These IB systems rely on a series of protective shells to protect the classified data. The combination of these shells provides the desired level of protection, but no individual shell has to provide perfect protection by itself. Because no individual shell is wholly responsible for data security, this layered system is not susceptible to single-point failure modes.



- No single-point failure modes
- Combination of protection methods
  - Elimination
  - Substitution
  - Hardware
  - Software
  - Procedures
- Series of **simple** protective shells
- Minimization of quantity of classified data

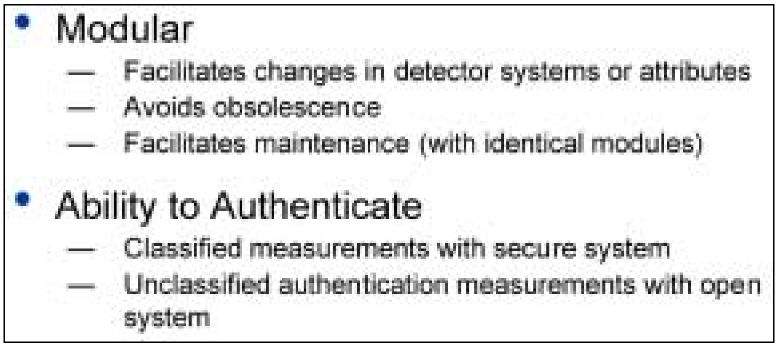
Fig. 3. Defense in depth.

Protection methods can include the following:

- elimination of potential leakage pathways (if classified data is not present in an element, then it cannot leak from that element);
- substitution of element types (e.g., fiber-optic links instead of wires};
- hardware protections (e.g., power-control relays and switches or discriminator settings);
- software protections (e.g., limitations in data-analysis programs); and
- procedural controls (such as written rules and requirements pertaining to allowable system operation).

The layered defense technique allows each layer to be relatively simple (hence more inspectable) while maintaining the desired overall level of security. It is anticipated that several different protection methods will be used in a final design. The demonstrated AMS/IB incorporated all five types of protection methods described above.

Other important design requirements (Fig. 4) include modular construction and the incorporation of open and secure modes to enhance the ability to authenticate the system.



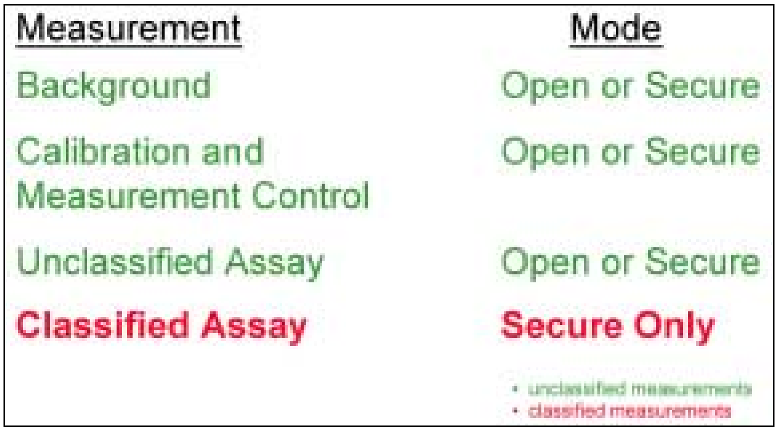
- Modular
  - — Facilitates changes in detector systems or attributes
  - — Avoids obsolescence
  - — Facilitates maintenance (with identical modules)
- Ability to Authenticate
  - — Classified measurements with secure system
  - — Unclassified authentication measurements with open system

Fig. 4. Other design requirements.

Modular construction implies that each major segment of the inspection system (e.g., each detector system and the integration control system) can be operated independently of the remainder of the system. Modular construction is nearly essential if different organizations are supplying parts of the inspection system from different locations. Other advantages of modular construction include the following.

- Authenticatability is greatly enhanced if the AMS/IB system is made up of a number of simple, single-purpose modules. If each module has only a single, well-defined, purpose, then extraneous capabilities are more easily detected.
- The construction team completely builds and tests each module before integration into the final system.
- Standard NDA detection systems can be used with a minimum of modification.
- Modular design facilitates future changes in detector design and/or attribute thresholds.
- If one module of the system becomes obsolete, it can be replaced without changing the remainder of the inspection system.
- If one module of the system fails, it can be replaced without having to replace the remainder of the inspection system.
- If many modules use identical elements (e.g., computer boards), a single stock of authenticated elements can be used to repair any one of the modules.

As mentioned above, the monitoring party must be able to authenticate these inspection systems. A primary method of authenticating an inspection system is to observe the complete operation of the inspection system when an unclassified source is being measured. The AMS/IB makes this possible by allowing operation in either the open or secure mode (Fig. 5). If the source is known to be unclassified, the AMS/IB can be operated with the doors open and monitors attached to each computer in the system. In this mode, background, calibration, and unclassified assay measurement can be performed with complete display of raw data, analyzed values, and pass/fail displays. In particular, the monitoring party can observe that the pass/fail display results match the data from the analysis computers.



Measurement	Mode
Background	Open or Secure
Calibration and Measurement Control	Open or Secure
Unclassified Assay	Open or Secure
Classified Assay	**Secure Only**

- unclassified measurements
- classified measurements

Fig. 5. ***Open vs secure modes of operation.***

In order to make measurements of classified items, the AMS/IB is placed in the secure mode. The monitor cables are removed, all access doors closed, and the pass/fail lights are the only output from the system. Only after the AMS/IB has been placed in the secure mode can measurements of classified items proceed. Measurements of unclassified items can be performed in the secure mode as well as the open mode, but measurements of classified items can only be performed in the secure mode (see the discussion of the security watchdog, Fig. 11).

The core information barrier concept (Fig. 6) consists of a secured area within protective shells.

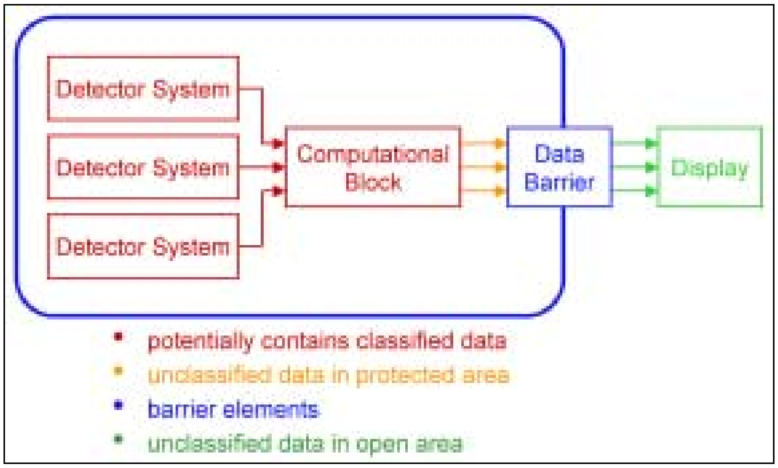
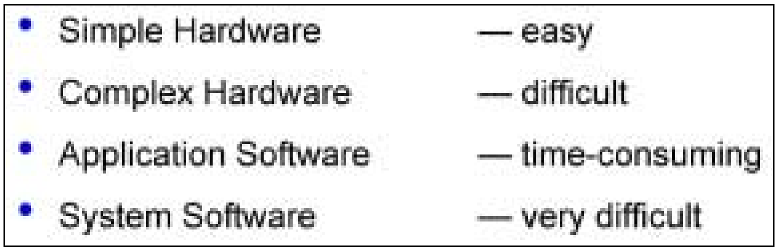

Detector System
Detector System
Detector System
Computational Block
Data Barrier
Display
potentially contains classified data
unclassified data in protected area
barrier elements
unclassified data in open area

Fig. 6. ***Core information barrier concept.***

All potentially classified information is enclosed by these shells. These potentially classified elements of the system include the detector modules and the computational block. Threshold comparisons are performed in the computational block so the outputs from this unit are the pass/fail answers that will eventually be displayed. These outputs are unclassified but are treated as classified due to their location within the secured area. These pass/fail results are passed out of the secured area through a data barrier (described in Fig. 11) to a simple display that is only capable of displaying pass/fail information.

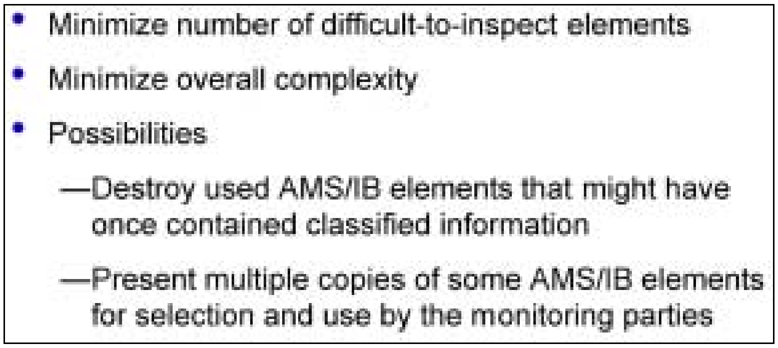
The design of the various elements in the AMS/IB takes into account the authentication/inspection requirements (Fig. 7). The element designs are based on the assumptions that simple systems are easier to inspect than complex ones and that hardware systems are easier to inspect than software ones. Thus the preferred solution (if possible) was always a simple hardware design, while complex system software was avoided.



• Simple Hardware	— easy
• Complex Hardware	— difficult
• Application Software	— time-consuming
• System Software	— very difficult

Fig. 7. Simplicity or difficulty of inspection of different types of elements.

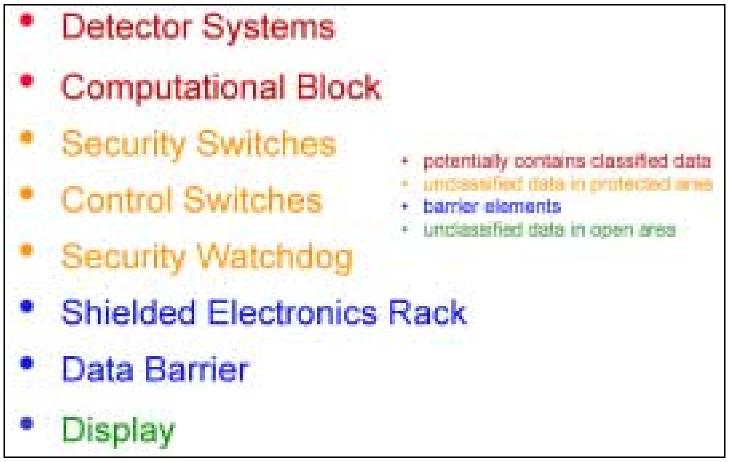
The ability to authenticate the AMS/IB (Fig. 8) was enhanced through the modularity discussed in Fig. 4 as well as several general design guidelines. The number of difficult-to-inspect elements (e.g., complex software) was minimized and the overall complexity of the AMS/IB was also minimized. All extraneous capabilities were removed. Procedural steps important in the authentication of the system would need to be negotiated on a regime-specific basis. Possibilities for such procedures could include destruction of computer-based AMS/IB elements rather than re-use, or presentation of multiple copies of key AMS/IB elements by the host country with a choice being made by the monitoring party. These, as well as other procedural authentication methods, were discussed in more detail in other presentations at the FMTTD. (Authentication of a Computer-Based System, and An Example of a Measure for Increased Confidence in Authentication).



- Minimize number of difficult-to-inspect elements
- Minimize overall complexity
- Possibilities
  - —Destroy used AMS/IB elements that might have once contained classified information
  - —Present multiple copies of some AMS/IB elements for selection and use by the monitoring parties

Fig. 8. Authentication considerations.

Thus, the entire AMS/IB (Fig. 9) was composed of (1) elements where classified information may temporarily reside (the detector systems and the computational block, see Fig. 10); (2) protective elements and "glue" elements (security watchdog and switches, data barrier, and electronics rack, see Fig. 11); and (3) input/output devices (the detector control switches and the unclassified display, see Fig. 12).

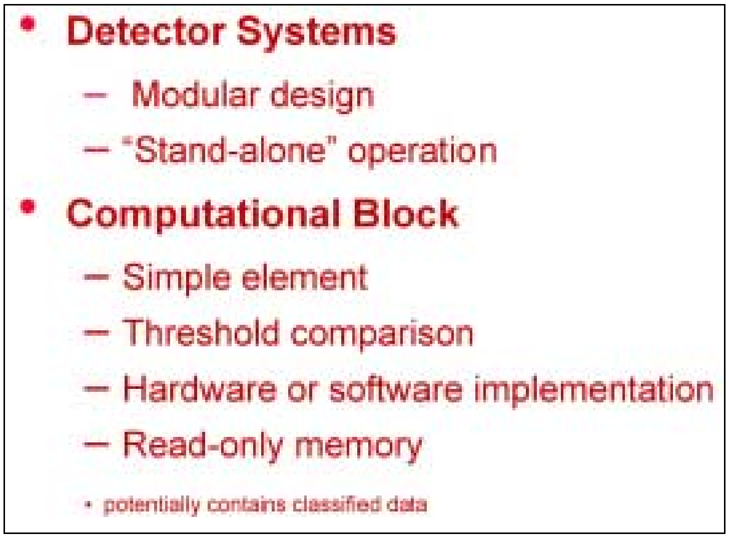


- Detector Systems
- Computational Block
- Security Switches
- Control Switches
- Security Watchdog
- Shielded Electronics Rack
- Data Barrier
- Display

- potentially contains classified data
- unclassified data in protected area
- barrier elements
- unclassified data in open area

Fig. 9. Entire AMS/IB system.

AMS/IB elements where classified information may temporarily reside (Fig. 10) include the detector systems and the computational block. As discussed earlier, the detector systems are designed to allow "stand-alone" operation and allow testing outside of the IB. Detector systems were covered in great detail in other presentations at the FMTTD. (Review of Plutonium Attribute Measurement Technologies, Physics Basis of the AMS/IB System, and Review of Plutonium Attribute Measurement Technologies: Neutron Measurements: Pu Mass & Absence of Oxide) The computational block is a simple element that performs the attribute threshold comparison. The computational block could theoretically be implemented in either hardware or software, although a software implementation was chosen for the AMS/IB. The computational block will boot independently and operates from a program stored in read-only memory (ROM).

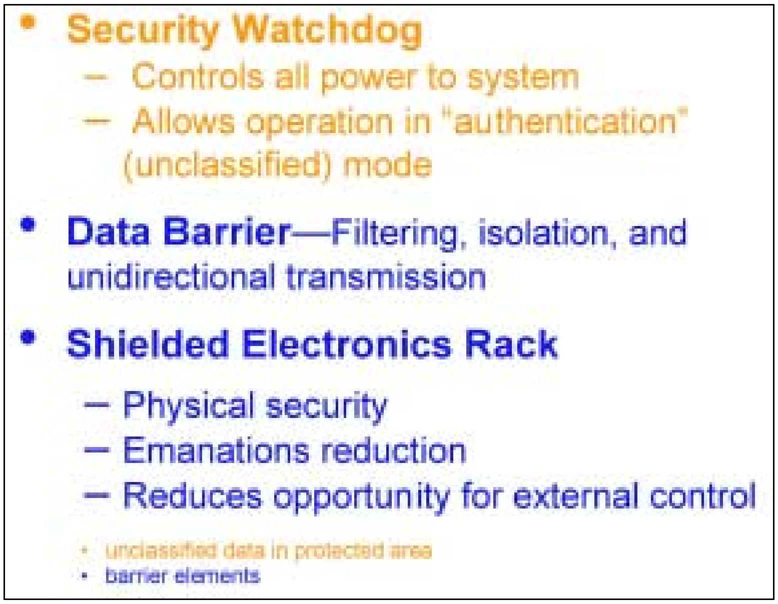


- **Detector Systems**
  - Modular design
  - "Stand-alone" operation
- **Computational Block**
  - Simple element
  - Threshold comparison
  - Hardware or software implementation
  - Read-only memory

- potentially contains classified data

Fig. 10. Elements that could contain classified information.

Protective measures (Fig. 11) include the data barrier, shielded electronics rack, and security system (watchdog and switches). The data barrier is the place where unclassified information is allowed to pass through the data barrier. This element will only allow a single output change per measurement cycle. In addition, data can only pass out of the electronics rack to the display (no input allowed) and isolation is provided between the classified areas within the cabinet and the unclassified display. The shielded electronics rack provides physical separation between classified data and unclassified output. In addition, it provides a measure of emanations reduction and reduces the potential for external control, manipulation, or tampering.



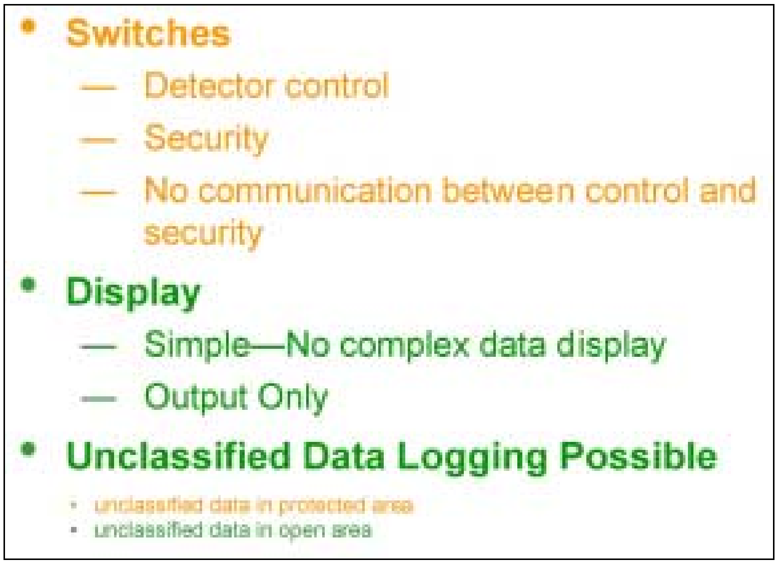
- Security Watchdog
  - Controls all power to system
  - Allows operation in "authentication" (unclassified) mode
- Data Barrier—Filtering, isolation, and unidirectional transmission
- Shielded Electronics Rack
  - Physical security
  - Emanations reduction
  - Reduces opportunity for external control

  - unclassified data in protected area
  - barrier elements

Fig. 11. AMS/IB protective measures.

All power to the remainder of the AMS/IB passes through the security watchdog. The security watchdog will allow the AMS/IB to function in the open mode only if an unclassified item is present in the measurement system. Security switches located in the detector cavity tell the security watchdog if a modified container is present. These switches were discussed in detail in another presentation at the FMTTD. (Technical Preview of the United States Demonstration of an Attribute Measurement System with Information Barriers).

The input and output devices (Fig. 12) are the only methods for interaction with the AMS/IB in the secure mode. The four data-control switches (background, gamma calibration, neutron measurement control, and assay) are used by the operators to start one of the four types of measurements of which the system is capable. Once the system has been started, no additional input is possible until a measurement is complete. After all measurements are complete, the output will display the appropriate lights: measurement complete at the end of a background or calibration measurement, failure if there is a failure within the AMS/IB, or attribute lights if an assay measurement has been performed. Note that if a failure occurs, no attribute lights will be illuminated.



- Switches
  - Detector control
  - Security
  - No communication between control and security
- Display
  - Simple—No complex data display
  - Output Only
- Unclassified Data Logging Possible
  - unclassified data in protected area
  - unclassified data in open area

Fig. 12. AMS/IB system input/output devices.

The interactions between all of these elements are shown in the system integration details (Fig. 13).

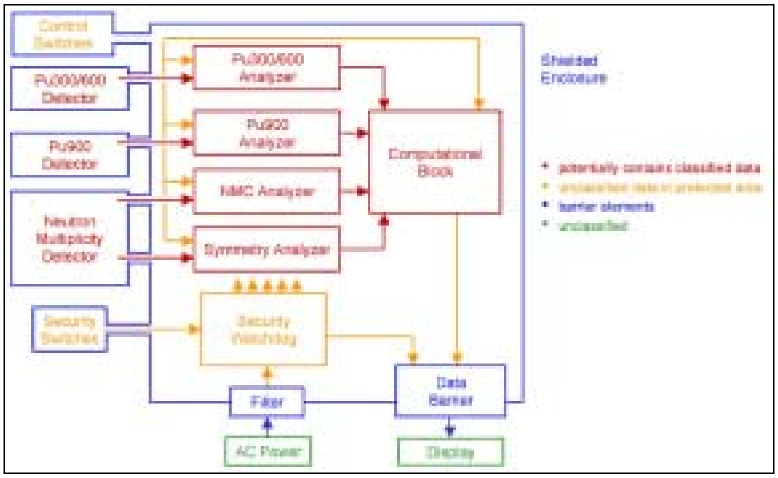
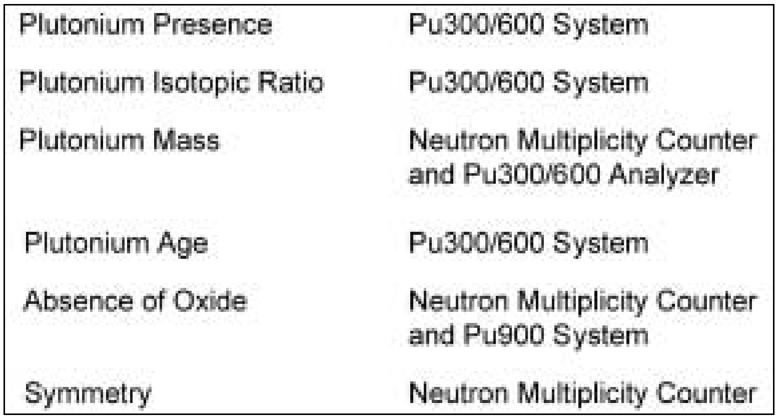


Fig. 13. AMS/IB system integration details.

Two important additional points are illustrated in this diagram.

- All software elements (four analyzers and the computational block) are contained within a hardware shell. Thus, malicious software cannot cause a breach in the barrier.
- The data-control switches and the security system are entirely separate. Thus, the data-acquisition system performs the same regardless of the security configuration. The analyzers do not know whether they are analyzing classified or unclassified data. This adds confidence that the measurement system will be the same whether a classified object or unclassified reference source is being assayed.

Finally, Fig. 14 lists the attributes measured by the AMS/IB; these are discussed in great detail in other FMTTD talks. (Physics Basis of the AMS/IB System and Sources and Thresholds for the United States Demonstration of an Attribute Measurement System with Information Barrier).



Plutonium Presence	Pu300/600 System
Plutonium Isotopic Ratio	Pu300/600 System
Plutonium Mass	Neutron Multiplicity Counter and Pu300/600 Analyzer
Plutonium Age	Pu300/600 System
Absence of Oxide	Neutron Multiplicity Counter and Pu900 System
Symmetry	Neutron Multiplicity Counter

Fig. 14. AMS/IB measured attributes.